Technical Cybersecurity

Moar Lab

Linux Debugging Tools

USING LINUX

- Linux (much) more prevalent in IoT
- Windows is more common in Enterprise computing

BINARY EXPLOITATION

- Focusing on linux techniques and systems

WE WILL

- …install a workstation
- …install debugging and hacking tools
- …install disassemblers/decompilers

Installing Linux VM

Ubuntu LTS

- You can install from ISO
- …or from OSboxes: https://www.osboxes.org/ubuntu/

We need tools!

- **$ sudo apt install gdb gcc binutils**
  - *GDB*: GNU Debugger
  - *GCC*: GNU Compiler Collection
  - *BinUtils*: GNU Binary Utilities

Python

Make sure you have Python

- `$ sudo apt install python python-pip`
  - …although you likely have python

Python3

- `$ sudo apt install python3 python3-pip`
  - …although you likely have python3

Python has nice tools for program argument manipulation

Hopper

DISASSEMBLER/DECOMPILER

- Links to GDB too, for a graphical debugger
- Free version (doesn’t have debugger links though)
- Download from: https://www.hopperapp.com

WE WILL LOOK OVER OTHER TOOLS TOO

- …and we can use them to look at disassembly too

Next, Binutils!